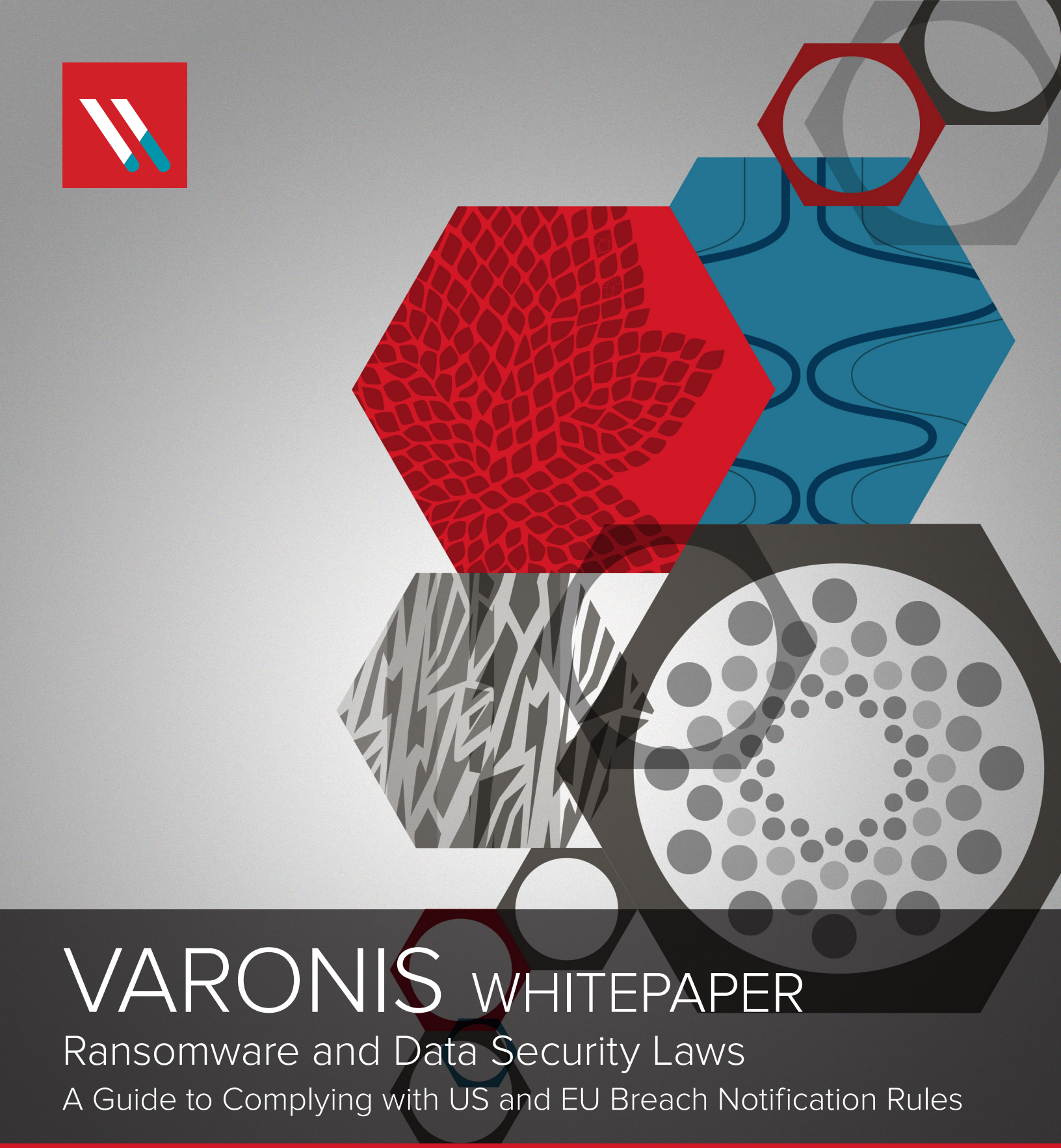


VARONIS WHITEPAPER

Ransomware and Data Security Laws

A Guide to Complying with US and EU Breach Notification Rules

CONTENTS

OVERVIEW ____ 3

RANSOMWARE 101 ____ 4

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ____ 6

- WHAT IS PHI ____ 6
- PLANNING FOR INCIDENTS ____ 7
- BREACH NOTIFICATION ____ 7

GRAMM-LEACH-BLILEY ____ 9

- FEDERAL TRADE COMMISSION ____ 10
- SECURITIES AND EXCHANGE COMMISSION ____ 10
- OTHER AGENCIES ____ 11

US STATE DATA BREACH LAWS ____ 12

EU DATA SECURITY LAWS ____ 13

CONCLUSION ____ 16

ABOUT VARONIS ____ 17

RANSOMWARE AND DATA SECURITY LAWS

A GUIDE TO COMPLYING WITH US AND EU BREACH NOTIFICATION RULES

Overview

Ransomware is a unique form of hacking in which data is not copied but left on site and encrypted. In a typical exploit, attackers scoop up or exfiltrate credit card numbers and other personally identifiable information (PII) to be then sold on the darkweb.

But digital extortionists instead directly ask companies for money and in exchange they'll decrypt the files that were made unusable. And that's only if they honor their word. Some paid the ransom, but didn't get all their files back. The cybercriminals demanded more money to decrypt the rest.

In the US, the Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPPA) are the most important federal-level laws for data security and privacy. At the state level, there are separate data security laws.

Are files that are accessed and encrypted by ransomware considered a data exposure by these laws — even when the data is not explicitly exported— and therefore requiring that affected individuals or parties to be notified?

In this paper, we'll try to answer this question.

As with any other malware, a financial or healthcare company that has been a victim of a ransomware attack could be out of compliance with respect to protecting the consumer data they're holding. For more information on overall data compliance considerations, refer to our Essential Guide to US Data Protection.

We'll be reviewing ransomware basics and then look into specific laws, principally HIPAA, GLBA, US state data laws, as well as the EU legal environment, with respect to their breach response requirements.

RANSOMWARE 101

Ransomware is a type of malware that infects computers and restricts users' access to their files by encrypting the file data. To release the file data, the victim is forced to pay a ransom and many pay just to keep the business going or because there was no recent backup.

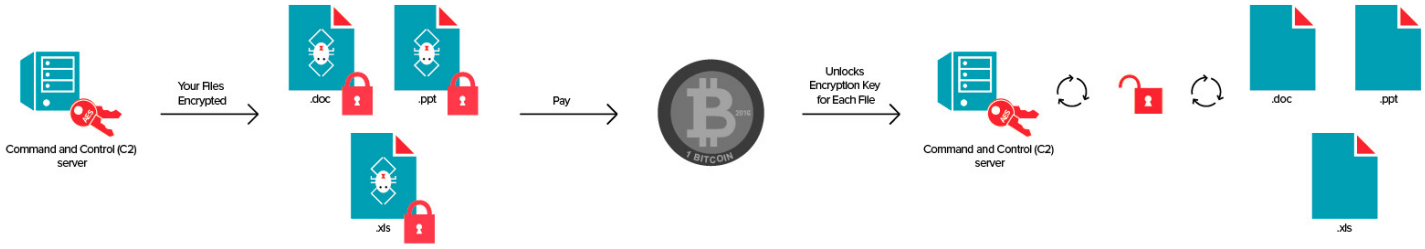
The actual mechanics of ransomware is relatively simple.

Let's take a look at Cerber, which is a typical ransomware variant.

With Cerber, an unsuspecting user clicks on a phish email attachment, in this case a Word document, and downloads it. The user then opens the doc, which launches a macro that ultimately starts the attack.

A hard-to-detect PowerShell script downloads the malware payload from the attackers Command and Control (C2) server. This malware—a binary executable, not a script — is also set to autorun on reboot, thereby making it persistent.

At this point, the heavy lifting is done by this evil executable, which traverses the file system, and encrypts each file with a different key (see diagram).



How does Cerber keep track of all the file encryption keys?

Simple: it appends the key used to encrypt each file to the end of that file, and then in turn encrypts that segment with a special key that is retrieves from the C2 server.

The attacker's servers effectively hold the key to the keys—the key that will unlock the specific encryption keys for each file.

And that's what you're really paying for when you send your bitcoins to the ransomer!

How much are organizations paying to get their files back?

In the well-known attack on Hollywood Presbyterian Medical Center, this hospital ultimately paid $17,000 in untraceable Bitcoins. The University of Calgary paid about $16,000 to get its emails decrypted.

According to the Department of Homeland Security, there have been over 300 cases of ransomware in 2015. More current information from the FBI provides an even more disturbing picture. They report that in 2016, ransomware infections on a global basis were at an all-time high.

Obviously, on its own a ransomware attack is a serious security incident. But regardless of whether your company pays the ransom, there can still be legal and regulatory implications in having this malware invade your file system.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA is the US federal law that covers health data privacy and security. More specifically, the regulators at the Department of Health and Human Services (HHS) wrote the Security Rule to protect health data, or in the language of HIPAA, protected health information (PHI).

WHAT IS PHI?

HIPAA doesn't explicitly define PHI other than to say it is information that can be "reasonably" linked back to an individual. To help health care organizations, HHS regulators devised a safe harbor rule: as long as health organizations and other covered entities protect the data in the following table, they would be in HIPAA compliance.

Names
All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes., except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census.
All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date.
Telephone numbers
Vehicle identifiers and serial numbers, including license plate numbers
Fax numbers
Device identifiers and serial numbers
Email addresses
Web Universal Resource Locators (URLs)
Social security numbers
Internet Protocol (IP) addresses
Medical record numbers
Biometric identifiers, including finger and voice prints
Health plan beneficiary numbers
Full-face photographs and any comparable images
Account numbers
Any other unique identifying number, characteristic, or code.
Certificate/license numbers

PLANNING FOR INCIDENTS

If a HIPAA covered entities (CEs)—hospitals or insurers -- or their business associates (BAs) – companies receiving PHI to process-- experience a ransomware attack, it would be considered a "security incident" under the Security Rule.

An incident is defined as follows:

"the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

A ransomware attack is then clearly a security incident. By the way, a HIPAA security incident doesn't have to involve PHI—it's any data that's been affected!

HIPAA's Security Rule then says that CEs and BAs should have a response program in place (45 CFR 163.308a6) when an incident happens. This includes, minimally, mitigating the damage and documenting the incident.

In the case of ransomware, where access to data is lost, the Security Rule further says that they must have a backup and recovery plan to meet contingency planning requirements (45 CFR 164.308a7).

BREACH NOTIFICATION

In 2009, a breach notification requirement was added to HIPAA as part of the HITECH law. It requires (45 CFR 164.400-414) CEs to notify affected individuals following the *"discovery of a breach of unsecured protected health information (PHI)."*

Translated into normal English, unsecured means unencrypted and breach means *"the unauthorized acquisition, access, use, or disclosure"* of PHI.

If you're following along, a breach is a subcategory of security incidents specifically directed at PHI.

The HIPAA breach definition covers our everyday understanding of this word – where data is copied or exfiltrated by the attackers—but it also includes mere access to the data.

Therefore, a ransomware attack that encrypts files containing PHI is a breach under HIPAA rules. Not only is it a breach, but it's also a security incident and therefore the CE (or BA) has to carry out its contingency plans (see above).

Let's focus now on what CEs have to do to respond to a breach notification.

On discovery of the ransomware and assuming that initial analysis show PHI was affected, the covered entity has to notify the affected individuals no later than 60 days in written form either by email or letter (45 CFR 164.404). The notification would have to include the description of the breach, the PHI that was involved, steps that should be taken by the victim to reduce harm, and what the CE is doing to investigate and mitigate risk.

For breaches affecting more than 500 individuals, the CE must notify HHS (45 CFR 164.408) and provide it with the same information as sent to individuals.

However, there are some additional subtleties in responding to a ransomware attack.

If the CE can show there's a "low probability" that PHI was affected, then it wouldn't have to report the breach.

For example, suppose an IT security group discovered the ransomware and stopped it, but not before it has affected a few directories where it's known – through a prior classification—that there's no PHI. In that case, the CE can say there's a low probability that PHI has been accessed and therefore would not have to notify consumers.

HHS has put out a helpful guideline explaining more of the complexities involved in a determination of a PHI breach.

In summary, a ransomware attack on a CE or BA would minimally involve implementing the response program to ensure continuity of operations, which would include recovery based on backups.

Beyond that, ransomware that affects PHI would require the CE to notify the affected individuals and the HHS when more than 500 records have been encrypted. BAs are required only to notify the CE (164.410) for which they are doing the work when their PHI has been encrypted by ransomware. The CE then in turn would directly notify the affected individuals and if need be, the HHS.

GRAMM-LEACH-BLILEY

Passed in 1998, Gramm-Leach-Bliley Act (GLBA) is an enormous piece of banking and financial legislation. The bill also contains signification data privacy and security requirements. Banks, brokers, mortgage companies, lenders, and financial advisers all fall under this law's data obligations.

GLBA protects nonpublic personal information (NPI), which is defined as any *"personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise 'publicly available.'"*

It is essentially ordinary PII—name, address, phone number, account number--with an exception for financial records—for example, property or certain mortgage information—that are required by law to be made public.

GLBA requires various federal agencies — including the Federal Trade Commission (FTC), the Federal Reserve, Treasury Department, and Securities and Exchange Commission (SEC) — to write their own specific data security regulations, known as safeguards rules, for protecting NPI: they need to *"establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information."*

FEDERAL TRADE COMMISSION

For its part, in 2002 the FTC regulators finalized their Safeguards Rule (16 CFR 314), which covers financial companies offering consumer lending and consumer investment advice.

These companies are required to have a program in place for *"detecting, preventing and responding to attacks, intrusions, or other systems failures."*

Is there an explicit breach notifications requirement in the FTC's regulation?

The answer is no.

However, the FTC has published a document on breach response guidelines for business. The FTC provided a series of recommendations — these are not requirements — that included having a response team of data forensic experts and legal advisers in place, as well as notifying law enforcement and affected individuals.

The other agencies covered by GLBA have come up with their own regulations.

SECURITIES AND EXCHANGE COMMISSION

In 2000, the SEC issued its data safeguards interpretation of GLBA known as Regulation S-P (17 CFR 248.30) for brokers, dealers, investment companies, and investment advisors.

Do the SEC safeguards regulations have a requirement for breach response and specifically breach notification?

Similar to the FTC's rules, companies falling under the SEC's GLBA related data regulations should have breach response as part of a security program, and issue breach notifications to relevant authorities and individuals. However, there are no explicit obligations for notifications, backups, and other disaster recovery measures.

OTHER AGENCIES

The regulators at the remaining agencies – Federal Reserve and Treasure Department —have been working out the details of their safeguards standards under GLBA.

In 2005, they jointly issued an Interagency Guidelines Establishing Standards for Safeguarding Customer Information

So are financial companies that are covered by these agencies—including bank holding companies, private bankers, and investment banks-- under explicit breach response and notification requirements for a cyber incident?

The answer is a qualified yes.

They have an "affirmative duty" to protect their customer's data against unauthorized use or access, and notifying the customers is *"a key part of that duty."* The company, though, first has to determine whether misuse of the information has occurred or is reasonably possible.

In the case of a ransomware attack, it's unclear from the regulations whether encryption alone is considered a misuse of data. If the financial company does send a notification under the Interagency Guidelines to customers, it would have to describe the incident, the data that was affected, and measures that were being taken to protect against further unauthorized access.

In short, the rules for a response to any kind of attack, let alone ransomware, launched against financial companies are not nearly as strict as for medical data. Keep in mind that these current regulations are subject to new interpretations—usually issued as guidances--and additional rulemaking by the regulators.

However, financial companies that inadequately respond to a ransomware attack could find themselves out of compliance with the spirit of GLBA's safeguards rules. It would be up to the individual regulatory agencies, and decided on a case by case basis whether to investigate and enforce the rules.

US STATE DATA BREACH LAWS

While the US currently doesn't have a general data breach notification law at the federal level, currently 48 states have their own laws.

This means that the basics of breach notification—what data is considered sensitive, what constitutes a breach, when and how consumers and agencies are notified—vary, sometimes greatly, depending on where a business collecting consumer data is located.

The state standards for notification are less rigorous than HIPAA. They lean towards a harm-based criteria for triggering an alert, and the list of personally identifiable information (PII) that's protected is far smaller – generally, name, address, phone number and auto license number, for example—than the federal health law.

More relevant to our discussion is whether a state considers mere access to PII to be a breach.

And here the list is quite small.

According to law firm Baker Hosteler's analysis, only two states fit this category: New Jersey and Connecticut. Puerto Rico, by the way, also considers the threshold for a breach to be *just* access.

However, both states also have a risk-of-harm analysis criteria: notification is not required if misuse of PII has not occurred or is not reasonably like to occur. However, in NJ a record of the analysis determination has to be kept for five years.

What misuse means here is a little unclear. Depending on circumstances, companies may not have to automatically report a ransomware attack to consumers in these two states.

The table below shows the PII used in each of these states notification laws. A company in these states that experiences a ransomware attack encrypting the relevant PII would have to notify affected individuals.

	PII	Exception	Notification	Risk of Harm Analysis
New Jersey	First name or first initial and last name and any one or more of the following data elements: (1) Social Security number; (2) Driver's license number or State identification card number. (3) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	PII is encrypted or made unreadable by other technical means.	Sent to NJ residents in the "*most expedient time possible and without unreasonable delay*" after discovery.	Yes. Record of analysis has to be kept for five years.
Connecticut	Same as NJ	Same as NJ	Sent to CT residents *"without unreasonable delay"* after discovery.	Yes

EU DATA SECURITY LAWS

Companies that do business in the EU have long had to deal with tougher and broader consumer data security and privacy laws that what we have in the US.

Since 1996, EU countries has been under the Data Protection Directive (DPD), which covers *"personal data"*— their word for PII — collected by companies from consumers. The DPD defines personal data as *"any information relating to an identified or identifiable natural person."*

Personal data is far closer in spirit to HIPAA's PHI, and in theory would cover traditional identifiers –name, address, phone number—as well as Internet-era handles, including email, IP address, and online user names.

The DPD acted as a kind of template, and EU countries were supposed to *"transpose"* the rules into specific national legislation. A country's local data protection authority (DPA) then enforces the law.

The DPD does *not* have a breach notification requirement.

However, a few EU countries, notably the Federal Republic of Germany, have added notification to their national data law. In Germany's case, though, a breach requires actual exposure of the personal data to a third party. This would imply that ransomware—if it only encrypts the personal data— does need to be reported.

In 2018, a revamp of the DPD, known as the General Data Protection Regulation (GDPR) will go into effect. Unlike the DPD, the GDPR will be a uniform law across the EU, and it includes a breach notification requirement.

According to the GDPR, a data breach is the *"accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

Under the GDPR, access alone is considered a breach and so ransomware that encrypts personal data would appear to require a notification to individuals and the relevant DPAs.

The details are spelled out in the GDPR's articles 33 and 34.

There is a 'but'.

On notifying the DPAs, the GDPR uses a harm threshold: no notification is required if the *"personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."* And the same threshold is applied when notifying the affected individuals.

Depending on the specific details of a ransomware attack, it could generally be argued that risks for consumers are low, and GDPR notification rules would not apply.

While we'll have to wait for clarification from the EU regulators, ransomware that can be shown not to exfiltrate any personal data would appear not to automatically require notification.

However, companies are required in the GDPR's article 33 to document the incident. And there are additional response requirements spelled out in article 32 ("security of processing"), including restoring availability and access to personal data.

For additional GDPR compliance information, please review our white paper on this new law.

Companies that do business in the EU or collect data from EU citizens remotely—through the new principle of extraterritoriality—will also be under the above obligations. In particular, US (and other foreign) e-commerce and social media companies that don't necessarily have an established presence in the EU would fall under the GPDR. These Internet-oriented companies should be closley following EU regulatory developments.

CONCLUSION

Ransomware clearly raises new issues for regulators, and starts pointing to the limitations of current consumer-oriented laws.

Under the two US federal laws discussed above, and the EU's new GDPR, there are circumstances where a severe ransomware attack that halted or severely limited operations would not require a notification to individuals or authorities.

At issue is the need for laws that deal specifically with cyberattacks that affect systems instead of malware that copies or access specific types of data.

The EU already is in the process of working out the rules for a cyberattack reporting framework. The US has a voluntary program for reporting cyberattacks to the Department of Homeland Security.

In any case, companies will need to defend against and reduce the risks of ransomware. Regardless of their actual legal response obligations, they should act as *if they will need to notify* customers and authorities, and have procedures in place to reduce further unauthorized access and restore data access.

We offer the following recommendations:

- **Data classification** Know where PII or personal data is stored on your file systems, especially in unstructured formats in documents, presentations, and spreadsheets.
- **Restrict access** Limit access to PII or personal data on a need-to-know basis or through role-based access controls. The goal is to make it difficult for attackers to access important data after hacking an ordinary user – say, through a phish mail—and launching ransomware based on that user's credentials. They should also remove and/or archive outdated or stale PII, further reducing the attack surface.
- **Monitoring** Since ransomware is essentially crawling a file system, navigating through each directory and examining files, it has a very distinct signature. Ordinary users whose credentials the ransomware is leveraging, do not perform these kinds of large-scale scans. Therefore, monitoring software, particular based on User Behavior Analytics (UBA), should be able to detect the ransomware and limit the number of files that are encrypted.
- **Backup and Recovery** Finally, companies should be regularly performing backups of their file system, especially critical and sensitive data, and have in place a recovery plan for restoring the data in the case of ransomware and other cyberattacks.

ABOUT VARONIS

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through an innovative software platform, Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search, and file synchronization and sharing.

All Varonis products are free to try for 30 days. Our systems engineering team will get you up and running in no time:

Fast and hassle free

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis — with concrete steps to improve your data security.

Fix real security issues

We'll help you fix real production security issues and build a risk report based on your data.

Non-intrusive

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

START YOUR FREE TRIAL